

# [***Exclusive: Biden officials confront limits of federal response in exercise preparing for 2024 election threats***](https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:6B94-67M1-JBSS-S00V-00000-00&context=1516831)

CNN Wire

February 9, 2024 Friday 5:00 AM GMT

Copyright 2024 Cable News Network All Rights Reserved

**Length:** 1661 words

**Byline:** By Sean Lyngaas, CNN

**Dateline:** (CNN)

**Body**

Washington (CNN) &#8212; When senior national security officials gathered in the White House Situation Room in December to prepare for the 2024 election, they faced a pair of stark, simulated scenarios that tested the limits of any federal response to election-related chaos, four people familiar with the meeting told CNN.

What if Chinese operatives created a fake AI-generated video showing a Senate candidate destroying ballots? And how should federal agencies respond if violence erupts at polling stations on Election Day?

For nearly an hour, the No. 2 officials at the FBI, CIA and departments of Homeland Security and Justice wrestled with how to respond to the deepfake video, including whether and how to notify the public about the activity if they weren't sure that China was behind it, the sources told CNN.

When it comes to a coordinated federal response to things like rampant disinformation, deepfakes and the harassment of election officials, "We're all f-king tied up in knots," said one US official familiar with the election security drill.

The previously unreported meeting was the first such drill the Biden White House has held in more than three years in office. It highlights the wrenching questions confronting the administration as it games out potential threats to the 2024 election -and the limits of federal power to respond to them.

US national security officials have to weigh whether publicly calling attention to disinformation might inadvertently amplify the very message they're trying to bat down. And they can act more swiftly to speak out publicly if they know that a foreign actor is behind an information operation targeting the election. If there's a chance an American citizen is involved, US officials are more reluctant to counter it publicly out of fear of giving the impression that they are influencing the election or restricting speech.

In both scenarios, federal officials favored a muted public response, largely choosing to let state and local governments take the lead. That points to a deep-seated dilemma they face: How does the federal government protect voters from election threats when many of those voters don't trust the federal government in the first place? State and local officials run elections and are more trusted voices in their communities, but how can federal officials act decisively to support them?

The participants opted for state election officials, and not the federal government, to lead any public messaging to counter disinformation spread by the fake video in their jurisdictions, two of the sources said. Officials also discussed options for notifying Congress. No one at the table raised their hand offering to be the lead federal agency to tell the public about the deepfake.

As for violence at the polls, the federal officials decided not to dispatch federal agents to support local police because they did not have the jurisdiction to do so.

'We're in uncharted territory right now'

The election security drill came the month after Chinese leader Xi Jinping [*assured*](https://www.cnn.com/2024/01/30/politics/xi-biden-china-us-2024-election/index.html) President Joe Biden in a face-to-face meeting that China would not interfere in the 2024 US election, signaling the administration was still preparing for that potential.

The role of deepfakes in election security has become all the more critical in light of the recent [*AI-made robocall*](https://www.cnn.com/2024/02/07/politics/biden-robocall-texas-strip-mall-invs/index.html) ahead of the New Hampshire primary that mimicked Biden's voice, another US official familiar with the meeting told CNN.

"We're in uncharted territory right now," said the first official familiar with the meeting, citing the ease with which someone can use AI to make fake audio and video to target voters and the challenges US agencies have in quickly responding. "It's the speed and the volume at which our adversaries can flood the information environment."

The Chinese Foreign Ministry said in a statement to CNN last week that China's position is to "always adhere to the principle of non-interference in other countries' internal affairs."

Officials from multiple federal agencies last week briefed the Senate Intelligence Committee on their election security preparation for 2024, including the White House drill in December, three sources familiar with the briefing told CNN.

There were pointed, unanswered questions about how the federal government will handle AI-generated fakes in the election, two sources said. And senators were left wondering how prepared the federal government truly is to respond to these kinds of threats.

A spokesperson for Senate Intelligence Committee declined to comment on the briefing.

"The election is already upon us and I'm going to keep pressing to make sure we're using all available resources and authorities to deter, detect, disrupt, and expose foreign efforts to meddle in our elections," Sen. Mark Warner, the Virginia Democrat who chairs the committee, said in a statement to CNN.

A senior administration official stressed that election security is a top priority in a statement to CNN.

"We remain concerned about a range of actors seeking to interfere in the electoral process and undermine confidence in our election infrastructure. Generative AI provides these actors a way to supercharge their malign efforts," the official said. "That's why there is a whole-of-government effort to ensure the integrity and security of the 2024 Federal elections."

Policies at the state level are also still a work in progress. CNN [*recently asked*](https://www.cnn.com/2024/02/01/politics/election-deepfake-threats-invs/index.html) election officials in all 50 states about efforts to counter deepfakes. Out of 33 that responded, most described existing programs in their states to respond to general misinformation or cyber threats. Less than half of those states, however, referenced specific trainings, policies or programs crafted to respond to election-related deepfakes.

In a recent interview with CNN, Francisco Aguilar, the secretary of state in Nevada, the state's top election official, said he is still working out how to deal with the threat of AI-generated fakes in elections and how federal agencies might be able to help him.

"You look at our budget at the state of Nevada and you see what constraints we have," Aguilar said. "I don't think we've been through a full election cycle where it's truly existed. So we are kind of in pioneering times right now."

Balancing vigilance with caution

After a relatively quiet midterm in 2022, federal officials tasked with election security are preparing for a range of potential threats, and are expecting hackers from Russia, China and Iran to be active, while viral conspiracy theorists are poised to pounce on any voting glitch to falsely cry fraud.

FormerPresidentDonald Trump's lies about voter fraud continue to resonate with large chunks of the country, with a majority of Republicans and Republican-leaners saying Biden's 2020 win was not legitimate, [*according*](https://www.cnn.com/2023/08/03/politics/cnn-poll-republicans-think-2020-election-illegitimate/index.html) to a CNN poll in July.

After getting caught flatfooted by a Russian hack-and-leak campaign in the 2016 election and by the pro-Trump rioters who stormed the Capitol after the 2020 election, US officials focused on securing the election are trying to balance the need to stay vigilant with being cautious about when to speak out about these threats without it backfiring.

Multiple former senior US national security officials involved in protecting elections told CNN that, in a post-2016 world, the disclosure of intelligence may be construed as political.

"It's a trick box," said Adam Hickey, who worked on election security issues for the Justice Department's National Security Division. "Unless the proof that it's a fake is virtually undisputable, [US officials] will be accused of weighing in on the election itself, and none of them want that."

But if US officials can expose the role of a foreign government in an interference campaign, Hickey said, "voters can weigh the message in light of its source, without speculating about who the foreign government favors or why."

Still scarred by 2016 Russian interference

Some in the federal government are still scarred by how slow the national security establishment was to warn the public about Russian interference in 2016. It was many months after the fact that states learned that Russian hackers had scanned their computer systems. But national security officials are also keen to avoid announcing a major new development on the eve of an election without giving the public adequate information to act on it.

During the White House drill, the senior federal officials were testing out a policy that was established after 2016 for notifying the public and Congress about foreign election interference. The policy stipulates that "partisan ***politics*** shall not play" a role in the decision to tell the public about foreign interference activities. It also asks officials to consider whether going public will render the foreign meddling less effective rather than inadvertently amplifying it.

The Justice Department, FBI and CIA declined to comment on the election security drill. The Department of Homeland Security referred questions to the National Security Council.

Cait Conley, a US Army combat veteran who joined DHS's Cybersecurity and Infrastructure Security Agency last year to bolster its election security work, declined to discuss the White House meeting but said her agency did over two-dozen security drills with state and local officials last year.

"[W]e prioritize tabletop exercises that integrate the range of cyber, physical, and operational threats election officials may encounter," Conley said in a statement to CNN. "Many of those threats are derived from the tactics and techniques of our foreign adversaries- from Chinese network penetration operations to Russian and Iranian foreign influence operations."

CNN's Evan Perez, Natasha Bertrand, Donie O'Sullivan and Katie Bo Lillis contributed to this report.

This story has been updated with additional information.

By Sean Lyngaas, CNN

TM & © 2024 Cable News Network, Inc., a Time Warner Company. All rights reserved.

**Load-Date:** March 8, 2024

**End of Document**